

SYSTEM AND METHOD FOR REMOTELY MONITORING
AND MANAGING APPLICATIONS ACROSS MULTIPLE DOMAINS

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority to U.S. Patent Application Serial No. 09/639,491, filed on August 15, 2000, entitled "COMPUTER-IMPLEMENTED SYSTEM AND METHOD FOR MONITORING AND MANAGING BUSINESS PROCESSES AND ASSOCIATED RESOURCES."

TECHNICAL FIELD OF THE INVENTION

This invention relates to the field of application monitoring and management, and more particularly to a system and method for remotely monitoring and managing applications across multiple domains.

TUSDO 175259/60

BACKGROUND OF THE INVENTION

Due to the increasing popularity and accessibility of the Internet, many traditional services have moved from the physical world to the Internet. For example, a multitude of Internet-accessible electronic marketplaces now exist and allow individuals and businesses to communicate and conduct transactions. Many such marketplaces are implemented using one or more applications that are executed on a computer system that is coupled to the Internet. To prevent unauthorized access to these enabling applications, the computer system supporting the applications often provides firewalls. In order to monitor and manage the operation of these applications to ensure the uninterrupted operation of the associated marketplace, a monitoring and management system may be executed on the computer system supporting the enabling applications. The owner of the computer system or another entity (such as the developer of the applications or an application service provider) may then use the monitoring and management system to monitor and manage the applications. Furthermore, an entity providing the monitoring and management service for one marketplace may provide the same service to one or more other marketplaces. However, unless that entity has been granted special access to the enabling applications through the firewalls of the associated computer systems, the entity may be required to locally monitor and manage the applications at each computer system. Such local monitoring and management may be an inefficient and complicated process.

DRAFT - DRAFT - DRAFT - DRAFT - DRAFT -

SUMMARY OF THE INVENTION

According to the present invention, disadvantages and problems associated with previous application monitoring and management systems and methods have been substantially reduced or eliminated.

According to one embodiment of the present invention, a system for enabling remote monitoring and management of one or more applications within a domain (the domain being one of a plurality of such domains) includes one or more computers within the domain which are coupled to a network. Each computer system executes one or more applications being monitored and managed. The system also includes a firewall that limits access to the applications within the domain from the network. The system further includes an application management layer within the domain that includes one or more agents that each monitor one or more corresponding applications and that generate notifications in response to the occurrence of events associated with the corresponding applications. The application management layer also includes a gateway that receives one or more of the notifications and stores the notifications in a database. In addition, the system includes a communication layer within the domain that retrieves one or more of the notifications from the database in response to a request received from a monitoring and management portal coupled to the network. The request is communicated to the communication layer using a communication protocol providing access through the firewall. The communication layer communicates the notifications to the monitoring and management portal using the communication protocol to enable remote monitoring and management of the associated applications.

According to another embodiment of the present invention, a method for remotely monitoring applications across a number of domains includes detecting the occurrence of events associated with a number of applications executed on a number of computers within the domains. Each domain is coupled to a network and includes a firewall that limits access to the applications within the domain. The method also includes generating notifications in response to the occurrence of the events (each notification being associated with at least one application) and storing at least some of the notifications in databases within the domains that include the associated applications. The method further includes retrieving notifications from the databases

PROVISIONAL DRAFT

of a number of selected domains in response to a request received from a monitoring portal that is coupled to the network. The request is communicated to the selected domains using a communication protocol that provides access through the firewalls associated with the selected domains. In addition, the method includes communicating the retrieved notifications from each of the selected domains to the monitoring portal using the communication protocol and making the retrieved notifications from each of the selected domains available at a computer associated with the monitoring portal for viewing in a unified manner.

According to yet another embodiment of the present invention, a method for remotely managing applications across a number of domains includes generating a command for each of a number of applications at a management portal that is coupled to a network. The applications are of a common type and are executed on a number of computers within the domains. Each domain is coupled to the network and includes a firewall that limits access to the applications within the domain. The method also includes communicating the commands to a communication layer within each of one or more selected domains using a communication protocol that provides access through the firewall associated with each selected domain. Each selected domain includes an application to which a command is directed. Within each selected domain, the method further includes communicating the command from the communication layer to an agent associated with the application to which the command is directed. The method also includes executing the command using a monitor within the agent that interfaces with the application.

The present invention provides a number of important technical advantages. For example, an application monitoring and management system is provided that allows an entity to remotely monitor and manage a number of applications that are executing on a number of different computer systems associated with a number of different domains. Through the use of hypertext transport protocol (HTTP) or other appropriate communication protocols, this remote monitoring and management capability is provided even when access to the applications is limited by firewalls. Embodiments of the present invention provide an application monitoring and management layer that interfaces with the applications and a communication layer that provides a remote monitoring and management portal with access to the

application monitoring and management layer (and thus the applications and information about the applications) through the firewalls protecting the applications. Therefore, the present invention allows the entity to monitor and manage a number of diverse applications from a single remote location and does not require that the entity be granted special access (for example, through the use of a virtual private network) to the computer systems supporting the applications through their associated firewalls. Furthermore, if appropriate, information from multiple domains may be aggregated and displayed to the entity in a single view to increase the efficiency of the monitoring and management process. Other important technical advantages are readily apparent to those skilled in the art from the following figures, descriptions and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

To provide a more complete understanding of the present invention and the features and advantages thereof, reference is made to the following description taken in conjunction with the accompanying drawings, in which:

5 FIGURE 1 illustrates an exemplary application monitoring and management system;

FIGURE 2 illustrates components of an exemplary application monitoring and management system in further detail;

10 FIGURE 3 illustrates an exemplary method for monitoring applications using a monitoring and management portal; and

FIGURE 4 illustrates an exemplary method for managing applications using a monitoring and management portal.

100-00000000000000000000000000000000

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 illustrates an exemplary application monitoring and management system 10. System 10 includes a network 12 that couples a monitoring and management portal 20 and one or more domains 30. Network 12 may include the Internet and/or any other network or combination of networks that may be used to couple portal 20 and domains 30. Portal 20 may be used to remotely monitor and manage one or more applications 42 executing at one or more computer systems 40 associated with one or domains 30. In an exemplary embodiment, domains 30 are data centers each executing one or more applications 42 that facilitate business-to-business (B2B), business-to-consumer (B2C), or other electronic marketplaces. However, applications 42 may include any appropriate applications providing any appropriate functions that may be monitored and managed using portal 20. For example, domains 30 may be business enterprises and applications 42 may be business processes, planning engines, or any other suitable applications executing at the various enterprises. One example of a system and method for monitoring and managing business processes is described in copending U.S. Application 09/639,491 filed August 15, 2000 (Attorney's Docket 020431.0565), which is incorporated by reference herein.

Each domain 30 may include multiple applications 42 that operate together to provide one or more services associated with domain 30, such as electronic marketplace services. However, a single domain 30 may include applications 42 providing multiple services and/or a single service may be provided using applications 42 executing in multiple domains 30. Furthermore, multiple domains 30 may be located at a single location, such as on a computer system associated with a data center, although such co-located domains 30 may be separated using firewalls or other security measures. Each domain 30 may be controlled by a different entity and still other management entities, such as may provide and/or monitor and manage applications 42 in one or more domains 30, such as application service providers (ASPs). Moreover, each domain 30 may include a firewall 50 that prevents unauthorized access to domain 30 through network 12.

Although domains 30 may be controlled and operated by various entities and applications 42 may be provided by other entities, a single management entity may be

TECHNICAL FIELD

5 assigned the responsibility of remotely monitoring and managing applications 42 executing in multiple domains 30. However, the management entity may not have access to domains 30 (through firewalls 50) or such access may be inefficient or impractical to obtain. System 10 provides the ability, using portal 20 and certain components that may be included in domains 30 (as described below), for a management entity to remotely monitor and manage a number of applications 42 executing in a number of different domains 30 even though those domains 30 may be protected by firewalls 50 and may reside at multiple physical locations. If appropriate, portal 20 may also be used to communicate simulated transactions to 10 applications 42 for monitoring purposes.

FIGURE 2 illustrates exemplary components of system 10 in further detail. Exemplary monitoring and management portal 20 includes a web browser 22 that may be used to communicate with domains 30 using HTTP or another communication protocol suitable to provide web-based communications between portal 20 and domains 30. The use of the term "HTTP" is meant to include HTTP, secure HTTP (S-HTTP), or any other communication protocol based on HTTP. However, any appropriate communication interface and/or communication protocol may be used to enable a user of portal 20 to receive information from domains 30 to monitor applications 42 and to transmit commands or other communications to domains 30 to 15 manage applications 42. Web browser 22 is coupled to a user interface 24 that provides the user with access to the information received at web browser 22 or other appropriate communication interfaces of portal 20 and that allows the user to transmit commands or other communications to domains 30. As an example only, user interface 24 may include a display for viewing information and a keyboard and a mouse to enter commands. Portal 20 also includes a repository 26 that may be used to 20 store user profiles and preferences. These user profiles and preferences may be used to customize the monitoring and management interface provided by portal 20 and the information gathered using portal 20 (for example, specifying which applications 42 at which domains 30 a particular user wishes to monitor and manage). Web browser 22, user interface 24, repository 26, and any other appropriate components of portal 25 30 30 may be provided using any appropriate combination of hardware and/or software and may be implemented on one or more computers at one or more locations.

As described above, each domain 30 includes one or more computer systems 40 executing one or more applications 42. Since domains 30 may be controlled by entities other than the management entity assigned to monitor and manage applications 42, and since domains 30 have associated firewalls 50 limiting access to applications 42, a communication layer 60 and an application monitoring and management layer 70 are included in each domain 30 to provide portal 20 with access to applications 42. Layers 60 and 70 are integral to or separate from one another and may be implemented using any appropriate combination of hardware and/or software executing on one or more computers.

Exemplary communication layer 60 includes a web server 62 and a servlet engine 64. Since typical firewalls 50 are configured (or may be readily reconfigured) to allow HTTP traffic to pass, portal 20 and communication layer 60 may communicate using HTTP or other suitable web-based communication protocols. Web server 62 and web browser 22 enable such HTTP communications between portal 20 and communication layer 60 (and firewall 50 passes any such communications). The use of HTTP or other similar suitable protocols simplifies communications between portal 20 and domains 30 and reduces or eliminates reliance on private or other special connectivity to domains 30. Furthermore, the use of a standard and relatively simple communication architecture such as HTTP allows system 10 to be readily modified and scaled. However, it should be understood that any appropriate communication technique may be used.

As described below, notifications or other information relating to applications 42 may be obtained and stored by application monitoring and management layer 70 in a database. In one embodiment, to communicate such information to portal 20, servlet engine 64 may be used to gather appropriate information from the database and to generate a web page or other appropriate content for communication by web server 62 to portal 20. Servlet engine 64 (such as a JRUN engine produced by ALLAIRE) executes servlets that are used to create this content. A servlet is a program, such as a JAVA program, that receives an HTTP or similar request, dynamically generates a response to the request, and communicates the response to web server 62 in the form of a hypertext markup language (HTML) file or other appropriate format (for communication to web browser 22). Like a common gateway

interface (CGI) script, servlets may query a database and generate content based on the results of the query. Servlets may also be used to receive commands in HTTP format from portal 20 and to communicate these commands (after any appropriate format conversion) to application monitoring and management layer 70. For example, a user of portal 20 may select a "link" on a web page to issue a command and a servlet may receive this selection and communicate the command to application management layer 70. Although the use of servlets and servlet engine 64 is described, any other appropriate method for obtaining information from application management layer 70 (such as CGI scripts or direct communication between web server 62 and application management layer 70) may be used.

Application management layer 70 is responsible for monitoring applications 42 and implementing commands received from portal 20. Application management layer 70 includes one or more agents 72 that may reside, for example, on the computer system 40 on which corresponding applications 42 being monitored are executing. Each agent 72 includes one or more monitors 74, which are managed objects (such as JAVA objects), that may be used to monitor or manage specific corresponding applications 42 or portions of such applications 42. For example, a monitor 74 may scan a log file produced by its corresponding application 42 to determine if selected events have occurred. The log file may document problems with application 42 and monitor 74 may scan for one or more problematic patterns reflected in the log file. Another monitor 74 may communicate with the same or a different corresponding application 42 to determine the state of the application 42 (for example, busy, idle, or not responding). Yet another monitor 74 may watch a communication port of the same or a different corresponding application 42. Monitors 74 may perform any appropriate monitoring and management functions. In an exemplary embodiment, agents 72 are JAVA Management Extensions (JMX) agents and monitors 74 are JAVA managed beans (MBeans); however, any appropriate agents 72 and monitors 74 may be used. One or more monitors, perhaps associated with multiple agents 72, may be used to monitor a single corresponding application 42.

Monitors 74 may generate notifications (or other similar messages) regarding events that have occurred in a monitored application 42 and may communicate these

notifications to the associated agent 72. Based on notifications received from monitors 74, an agent 72 may take actions to notify a user of portal 20 about a problem with an application 42 or take appropriate action to remedy the problem. For example only and without limitation, an agent 72 may send e-mail or pager alerts to appropriate parties, log notifications to a database 76, or restart an application 42 that has failed. Agent 72 may use a gateway 78 to log notifications to database 76. In one embodiment, events service 80 provides the capability for a user of portal 20 to subscribe to particular notifications from monitors 74, such as notifications of state changes for a particular application 42 or an alert regarding an application 42. Based on a subscription to particular notifications with events service 80, gateway 78 receives and forwards appropriate notifications from agent 72 to database 76 (where the notifications are stored for later retrieval by servlet engine 64, as described above). Furthermore, gateway 78 may forward notifications to other management clients, such as a Simple Network Management Protocol (SNMP) manager.

Application management layer 70 also includes a system manager 82 that provides an interface for a management entity to interface with and control agents 72 and other components of application management layer 70. In an exemplary embodiment, system manager 82 may include a JMX manager. Although a single computer system 40 is illustrated, system manager 82 may be used to provide an interface to agents 72 associated with multiple computer systems 40 in a domain 30. System manager 82 acts as a broker for agents 72 and enables communications between a management client, such as portal 20, and agents 72. In one embodiment, system manager 82 provides public application program interfaces (APIs) that allow portal 20 to interact with agents 72 and to subscribe to notifications using events service 80. For example, using an agent API, portal 20 may command an agent 72 to start, stop, or modify the operation of an application 42, may instruct an agent 72 to log particular events associated with an application 42, and may configure an agent 72 to operate in any other suitable manner. System manager 72 may also monitor the other components of application management layer 70 to ensure that they are functioning properly.

Application management layer 70 further includes a dynamic lookup service 84 that provides a dynamic registry where agents 72 and any other components of

application management layer 70 may register and unregister. System manager 82 may use this dynamic lookup service 84 to identify an agent 72 and to establish communications between an agent 72 and portal 20. Dynamic lookup service 84 also provides a "heartbeat" service by monitoring agents 72. If an agent 72 terminates normally or abnormally, dynamic lookup service 84 unregisters the agent 72 and notifies system manager 82 or any other appropriate entity (such as portal 20) that corrective action may need to be taken. Application management layer 70 also includes a security service 86 that provides a permissibility mechanism which ensures that only authorized users or clients are able to access particular components of application management layer 70. The various components of application management layer 70 described above, including agents 72 and associated monitors 74, may be remote from or embedded in applications 42 being monitored and managed. Furthermore, these components may be implemented using any appropriate combination of hardware and/or software associated with one or more computers at one or more locations.

In many cases, the same management entity (such as an ASP) may provide monitoring and managing services for multiple domains 30. For example, an entity may be hired to monitor and manage the operation of multiple electronic marketplaces implemented using applications 42 in multiple domains 30 or the operation of business processes in domains 30 associated with multiple enterprises. Without the use of the present invention, such a management entity may be required to operate monitoring and management systems locally at each domain 30 if the entity does not have direct access to applications 42 due to the presence of firewalls 50. However, the use of communication layer 60 and application management layer 70 in a domain 30 allows the management entity to monitor and manage a number of domains 30 from a single remote location (portal 20) and does not require that the entity be granted special access (for example, through the use of a virtual private network) to the domains 30 through their associated firewalls 50. Furthermore, if appropriate, information from multiple domains 30 may be aggregated and displayed to a user of portal 20 in a single view to increase the efficiency of the monitoring and management process.

FIGURE 3 illustrates an exemplary method for monitoring applications 42

using portal 20. The method begins at step 102, where a user of portal 20 configures one or more agents 72 and monitors 74 to monitor selected applications 42 in one or more domains 30. As described above, the user may configure agents 72 and monitors 74 using HTTP communications and one or more APIs provided by system manager 82 or other components of the associated application management layer 70. At step 104, the user may also configure custom views or displays so that selected information may be obtained and displayed by web browser 22 and user interface 24 in a desired format. The user may then initiate the monitoring of the selected applications 42 at step 106 by issuing one or more commands to application management layers 70 of the selected domains 30.

At step 108, the selected monitors 74 detect the occurrence of events relating to applications 42. For example, a first monitor 74 may communicate with its corresponding application 42 to determine the state of the application 42 and a second monitor 74 may scan a log file associated with the same or a different corresponding application 42. Monitors 74 report detected events to their respective agents 72 though the communication of notifications to the agents 72 at step 110. Although the detection and notification of events is illustrated as two steps in a sequence of steps, it should be understood that detection and notification may occur substantially continuously during the operation of system 10. At step 112, an agent 72 that has received a notification from an associated monitor 74 communicates the notification to gateway 78 for storage in database 76. As described above, agent 72 may also communicate the notification to a user as an e-mail, or pager or other message and/or to another management client. Agent 72 may modify the content or format of a notification received from a monitor 74 as appropriate for the intended recipient of the notification.

At step 114, a servlet executed by servlet engine 64 queries database 76 to retrieve selected notifications. This query may be performed on a periodic basis or at selected times, in response to the selection by a user of portal 20 of particular applications 42 or types of events that the user desires to be monitored (for example, through the customization of a display), in response to a current request by the user for an update with respect to particular events or applications 42, or for any other appropriate reason. As described above, the servlet may generate an HTML response

or other appropriate content including the notifications (although they may be in modified form) to web server 62. Web server 62 communicates the notifications through firewall 50 to portal 20 at step 116. These notifications may be sent using HTTP or any other appropriate communication protocol. At step 118, web browser 22 receives the notifications (in the form of an HTML page or other appropriate content) and the notifications are displayed to a user of portal 20 using user interface 24. The notifications may be modified as appropriate for display to the user (for example, in a graphical format). The user may then take appropriate actions based on the notifications. Therefore, embodiments of the present invention allow the management entity to monitor and manage a number of domains 30 from a single remote location (portal 20) and do not require that the entity be granted special access to the domains 30 through their associated firewalls 50. Furthermore, if appropriate, information from multiple domains 30 may be aggregated and displayed to a user of portal 20 in a single view to increase the efficiency of the monitoring and management process.

FIGURE 4 illustrates an exemplary method for managing applications 46 using portal 20. The method begins at step 132, where a user of portal 20 communicates a command or other appropriate message for an application 42 to a web server 62 (or any other appropriate component) of a domain 30. The command may be communicated by the user in response to the receipt of a notification relating to an application 42 or for any other appropriate reason. As an example only, the command may instruct a particular application 42 to restart after the user has received a notification that the application 42 has failed. The command may be communicated to web server 62 using HTTP or any other communication protocol allowing the communication to pass through the firewall 50 of the domain 30.

At step 134, the command is received by the web server 62 and web server 62 communicates the command to the one or more agents 72 associated with the one or more applications 42 to which the command is directed. Web server 62 may modify the content or format of the command as appropriate for the receiving agent 72 (for example, according to an API provided by system manager 82 for the agent 72). The agent 72 receiving the command instructs one or more monitors 74 to execute the command or otherwise act upon the message from portal 20 at step 136. Agent 72

may determine an appropriate monitor 74 to execute a command based on the monitor's assigned interaction with the application 42 for which the command was given. At step 138, one or more monitors 74 execute the command or act upon the message as instructed by corresponding agents 72. Therefore, embodiments of the present invention allow the management entity to communicate commands to applications 42 in a number of domains 30 from a single remote location (portal 20) and do not require that the entity be granted special access to the domains 30 through their associated firewalls 50.

5

10

Although the present invention has been described with several embodiments, numerous changes, substitutions, variations, alterations, and modifications may be suggested to one skilled in the art, and it is intended that the invention encompass all such changes, substitutions, variations, alterations, and modifications as fall within the spirit and scope of the appended claims.

100-00000000000000000000000000000000